Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-16. (Canceled)

17. (Currently amended) An optical disk playing system comprising:

a plurality of downloadable external media content provided on one or more computing devices distributed on a network, each downloadable external media content having been added with a private key;

an optical disk comprising internal media content associated with the external media content and a public key to verify the authenticity of each of the external media content;

an output for playing the internal media content in coordination with the associated authenticated external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided.

18. (Previously presented) The optical disk playing system according to claim 17, wherein the public key is stored in a BCA (Burst Cutting Area) zone of the optical disk.

19. (Previously presented) The optical disk playing system according to claim 17, wherein

the public key is stored in a media content zone of the optical disk.

20. (Currently amended) An optical disk player comprising:

an optical disk driver unit to read-out internal media content and a public key, both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content;

a network interface to download one or more external media content, each external media content having been added with a private key and is provided on one or more computing devices distributed on a network;

a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk; and

an output portion to output the internal media content in coordination with the associated downloaded authenticated external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided.

21. (Previously presented) The optical disk player according to claim 20, wherein the control system detects whether the downloaded external media content is integral before verification, wherein said verification will not be executed if the downloaded external media content is detected to not be integral.

22. (Previously presented) The optical disk player according to claim 20, wherein the downloaded external media content is an application program.

23. (Previously presented) The optical disk player according to claim 22, wherein the application program is a JAVA language application program.

24. (Previously presented) The optical disk player according to claim 20, wherein the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to the private key of the downloaded external media content.

25. (Currently amended) A method for playing an optical disk, comprising acts of:

reading-out internal media content and a public key, both provided on a same optical disk, the public key is to verify authenticity of external media content associated with the internal media content;

downloading from one or more computing devices distributed on a network one or more external media content having been added with a private key;

verifying the authenticity of each of the downloaded external media content using the public key read-out from the optical disk; and

outputting the internal media content in coordination with the one or more associated downloaded authenticated external media content,

wherein the authenticity of the external media content is verified independent of the

authenticity of one or more computing devices on which the external media content is provided.

26. (Previously presented) The method according to claim 25, further comprising acts of:

detecting if the downloaded external media content is integral; and

executing the verifying act only if the downloaded external media content is detected to be integral.

27. (Previously presented) The method according to claim 25, wherein the coordination between the read-out internal media content and the downloaded external media content will not be established if the downloaded external media content is not authenticated.

28. (Previously presented) The method according to claim 27, wherein the coordination between the read-out internal media content and downloaded external media content will be established if the downloaded external media content is authenticated.

29. (Previously presented) The method according to claim 25, wherein the downloaded external media content is an application program.

30. (Previously presented) The method according to claim 29, wherein the application program is a JAVA language application program.

31. (Previously presented) The method according to claim 25, wherein verifying the authenticity of the downloaded external media content comprises an act of performing asymmetric cryptography using the public key read-out from the optical disk corresponding to the private key of the downloaded external media content.

32. (Previously presented) The method according to claim 25, wherein the optical disk comprises digital information stored thereon, the stored digital information comprising network address information that is used to download the external media content and the public key that is used to verify the authenticity of the downloaded external media content before playing the internal media content in coordination with the external media content.